ABSTRACT OF THE DISCLOSURE

   In a modular arithmetic apparatus including a
plurality of product-sum circuits having a modular
arithmetic function and parallelly arranged, and a
5   correction term calculation unit for calculating a
correction term to be used for modular arithmetic
operation in the product-sum circuits, the correction
term calculation unit sequentially calculates the
correction term in units of bits, and each of the
10   product-sum circuits sequentially reflects the
correction term calculated by the correction term
calculation unit and performs base conversion or base
extension.